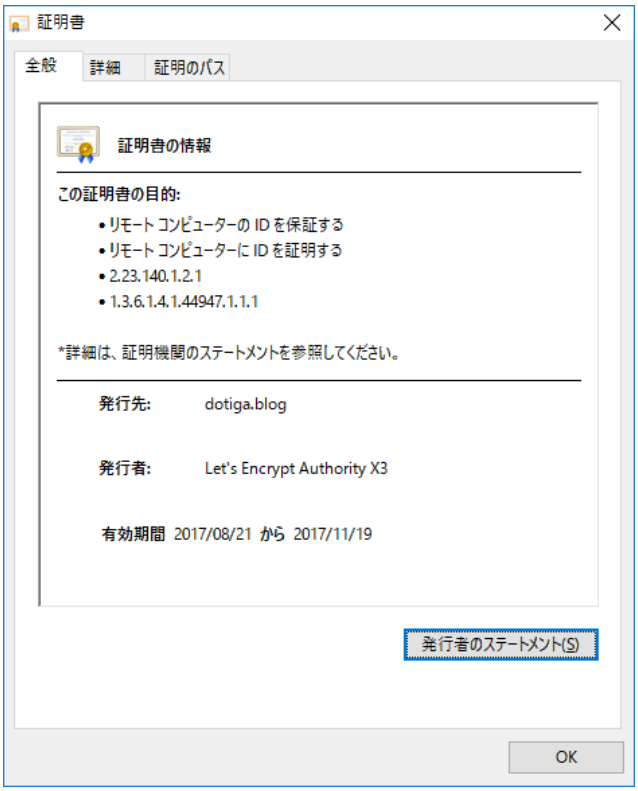
【無料の SSL サーバー認証局 Let's Encrypt の利用方法　Rev.0.9】

無料で簡単に常時 SSL 化を
Google の検索順位を優位に！！



どっといが（五十嵐 康雄）

改訂履歴			
Rev.	日　付	改 訂 内 容	備 考
0.9	2017 年 11 月 18 日	新規作成	

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

はじめに

このレポートの利用に際しては、以下の条件を遵守されるようお願い申し上げます。

このレポートに含まれる一切の内容に関する著作権は、レポート作成者に帰属し、日本の著作権法や国際条約などで保護されています。

著作権法上、認められた場合を除き、著作権者の許可なく、このレポートの全部又は一部を、複製、転載、販売、その他の二次利用行為を行うことを禁じます。
これに違反する行為を行った場合には、関係法令に基づき、民事、刑事を問わず法的責任を負うことがあります。

レポート作成者は、このレポートの内容の正確性、安全性、有用性等について、一切の保証を与えるものではありません。また、このレポートに含まれる情報及び内容の利用によって、直接・間接的に生じた損害について一切の責任を負わないものとします。

このレポートの使用に当たっては、以上にご同意いただいた上、ご自身の責任のもとご活用ください。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

まえがき

この度は、どっといがのレポート

【無料の SSL サーバー認証局
Let's Encrypt の利用方法 Rev.0.9】
無料で簡単に常時 SSL 化を
Google の検索順位を優位に！！

をダウンロードしていただきまして、ありがとうございます。

Google の「**常時 SSL**」の推奨とか、
SSL サーバー証明書を無料で取得できる Let's Encrypt のサービス開始などで、
常時 SSL 化の波が大きくなっています。

本レポートは、ご自分で Web サーバーを開設されている方に向けて書いたものです。

共用型のレンタルサーバーを利用されている方は、
Google Ad Sense など SSL 化対応の広告コード貼り付けの記事が参考になるかと思いますが、無料や有料の商用ブログサービスでブログを開設されている方は対象外です。

本レポートでは、以下の 2 点について整理してあります。

(1) Let's Encrypt での無料の SSL サーバー証明書の取得と、
Web サーバーへの設定について（**CentOS 7/Apache 2.4**、他の Web サーバーについてはご容赦を！）

(2) Web ページに貼り付ける、下に示す ASP の広告コード SSL 対応状況について
- Google AdSense
- Amazon アソシエイト
- A8 ネット

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

・その他

ページに SSL 非対応のリンクが挿入されていると、そのページは保護されたページにはなりません。
広告収入を得ようとしている方にとっては、大きな関心事です。

実際に SSL 化を実施してみると、想像していたものよりはるかに簡単です。
Let's Encrypt 利用すれば、誰でも挫折することなく「**常時 SSL**」が実現できるものと思います。

今更「**常時 SSL 化**」の方法？
と本レポートを出すには遅くなってしまった感は否めません。

でも、これからという方！
本レポートを参考に、あなたのサイトを**常時 SSL** 化に対応してみてください
（実は、私もレンタルサーバーの方のサイトの対応は未だなんです。
自前構築の自宅サーバーのみ対応）。

Google などの検索サイトからの評価が上がるようになるように、本レポートが少しでもお役にたてればと思います。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

本レポートをダウンロードしていただいたお礼として
耳寄りな情報をご案内したいと思います。

【無料】

最高のプレゼント！
PDF ファイル 1,500 ページ、動画１３時間！！

※ プレゼントのお受け取りは、「プレゼントアイコン」をクリックしてくださいネ

また、今まで通り、

これからアフィリエイトを始める上で、
マインドやスキルを上げるために必須な情報が書かれた
PDF ファイルとセミナー動画を 6 本

もこちら↓からお受け取りできます。

⇒ http://dotiga.jp/present/specialpre.zip

ユーザー名: iwat
パスワード: aMio

このプレゼントを作成してくださったのは、
「五十嵐 友」という方です。

五十嵐友先生は、
トップアフィリエイターとしての実績を残され、

現在無料のアフィリエイト塾【フレンドマーク】を
運営されていらっしゃいます。

⇒ フレンドマーク塾

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

本レポートをダウンロードされた方は、
わたしのニュースレター（情報商材紹介のメルマガではありません）

『アフィリで稼ぐためのソフトウェア』

に代理登録させていただくことをご承知おきください。

ご不要の時は、巻末に示してある URL から解除できます

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

目次

1　概要 1

2　SSL/TLS 2

2.1　常時 SSL 3

2.2　SSL/TSL とは? 4

2.3　SSL サーバー証明書 7

2.3.1　SSL サーバー証明書の種類（ドメイン認証・企業認証・EV 認証） 8

（１）　独自 SSL と共有 SSL 8

（２）　独自 SSL の種類 9

2.3.2　SSL サーバー証明書の確認方法 10

（１）　Google Chrome 最新バージョン 10

（２）　Windows10 の標準ブラウザである Microsoft Edge。 13

3　無料で利用できる SSL 証明書 Let's Encrypt 14

3.1　Let's Encypt とは？ 15

3.2　Let's Encrypt の利用手順 17

3.2.1　事前に行っておくべきこと 18

3.2.2　Certbot クライアントのインストール 19

3.2.3　SSL サーバー証明書の作成 20

（１）　certbot クライアント 20

（２）　SSL サーバー証明書が保存される場所 25

3.2.4　Apache 2.4 への設定 27

3.3　SSL 証明書の自動更新 28

4　AdSense、その他の広告コードの SSL 化対応 29

4.1　AdSense 用広告コード 30

4.2　その他の広告コード 32

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

1 概要

Google より、「常時 SSL」が SEO 対策へ及ぼすことがアナウンスされています。

HTTPS をランキング シグナルに使用します

自分のサイトでビジネスを行っている人なら、ほっておけない問題なのかもしれません。

常時 SSL とは、
一口でいうと Web サイトの全ページを HTTPS 化（SSL/TLS 暗号化）するセキュリティ手法のことです。

自分のサイトを HTTPS 化にするには、「SSL サーバー証明書」というものが必要となります。
従来、SSL サーバー証明書は購入する価格が安くはなく、また簡単な手続きで購入できるものではありませんでした。

でも、2016 年 4 月 12 日に完全無料で「SSL サーバー証明書」が取得できる Let's Encrypt というサービスが開始されて、少なくとも費用の面からの困難が解消されました。

実際に利用してみると導入手続きや Web サーバーへの設定等、想像以上に簡単で、
SSL 導入への敷居を大幅に低くするものです。

本書は、その Let's Encrypt の利用の仕方を中心に、心配な Web ページへの広告貼り付けの話を中心に記述します。

参考までに、一番簡単なドメイン認証型の SSL サーバー証明書を取得する一般的な流れは、以下に示す通りです。

(1) 秘密鍵を作成
(2) 秘密鍵を元に、CSR（証明書を発行するための署名要求）を生成
(3) 認証局へ CSR を送信
(4) 認証局からドメイン所有者へ確認メールが届くので承認する
(5) 認証局から証明書がメールなどで届く

Let's Encrypt の場合は、Let's Encrypt クライアントソフト(コマンド)をインストールして、証明書を取得するためのコマンドを打つだけなのです。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

2 SSL/TLS

本章では、「**常時 SSL**」の背景である SSL/TLS について、ざーっと説明します。

知識がお有りの方は、読みとばされて全く問題はありません。

『「**常時 SSL**」の細かい背景は難しそうだ』と思われる方は、軽く眺めてください。

本章の内容だけで常時 SSL の技術的背景を深くご理解いただけるのは容易なことなく、利用するだけならそれほど深く理解する必要もないでしょう。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

2.1　常時 SSL

Web サイトのすべてのページを暗号化（SSL/TLS 化）することを、
常時 SSL（Always On SSL）といいます。

常時 SSL は、Web サイト内のログインページやフォームなど特定のページだけでなく、
その他すべてのページを **SSL/TLS 化**することで、ログイン情報や決済情報だけでなく、
Cookie への不正アクセス（盗聴）も防止することができます。

SSL/TLS 化された Web サイトは、URL の頭が「HTTPS」となり、
通信の暗号化が保証されます。

これにより、
ユーザーは安心して Web サイトから個人情報や決済情報を提供することができ、
第三者による盗聴を心配する必要がなくなります。

さらに、企業実在認証付きの証明書や EV 証明書がサイトに入っている場合には、
アクセスしている Web サイトに証明書が入っていることが確認できるため、
擬似サイトやなりすましサイトへの誘導を防ぐことができるといったメリットがあります。

常時 SSL 化するメリットに、
検索エンジンから「ユーザーが安心して利用ができる優良なコンテンツである」と評価されることが挙げられます。

モバイルデバイスの普及により、
「いつでもどこでも」Web サイトを閲覧したり、
Web サービスや検索エンジンを利用する頻度が増えている昨今、
自社の Web サイトやサービスを利用するユーザーが、
フィッシング詐欺や盗聴などの被害に遭わないようにするために、Web サイト自体の安全性の向上がより一層求められています。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

2.2 SSL/TSL とは?

では、**SSL** とは、いったいどんなものなのでしょうか？

SSL（Secure Socket Layer）とは、
インターネット上でデータを暗号化して送受信する方法のひとつで、
Netscape Communications 社が開発しました。

今でこそ Web ブラウザといえば Internet Explorer や Google Chrome などがよく知られていますが、
1995 年前後は **Netscape Communications** 社が開発した Netscape Navigator がシェア一位でした。

TLS は、**SSL** と大枠の仕組みで同じものです。

SSL がバージョンアップを重ねて「SSL3.0」となり、
その次のバージョンから「TLS1.0」という名称で呼ばれるようになりました。

SSL の名称はインターネットユーザーの間で広く普及しているため、
TLS を指していても、SSL または SSL/TLS と表記することが多くなっています。

本書でも暗号化通信の技術自体を指す場合は「SSL/TLS」、
SSL/TLS 技術を利用した電子証明書の呼称は一般のネットユーザに分かりやすいよう
「SSL サーバー証明書」と記述することにします。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

通常、インターネットでは、データが暗号化されずに送信されています。
そのため､通信途中でデータを傍受されると､情報が第三者に漏れてしまう可能性があります。

また、相手のなりすましに気づかずに通信すると、
データがなりすましの相手に取得されてしまう可能性があります。

表 2.2-1 電子商取引におけるリスク

なりすまし	なりすましとはサイトの運営者や、関係者等相手になりすますことです。 例えば、EC サイト運営者になりすまし、 クレジットカードの番号や住所等の顧客情報等を取得し、悪用したりします。
盗聴	情報の送信元と送信先以外の第三者により、情報を盗み見られること。 EC サイト等で個人情報のやりとりを行っている際に盗聴されると、 住所やクレジットカード番号等が漏れてしまいます。
改ざん	情報の送信元と送信先以外の第三者により、情報の内容を書き換えられること。 EC サイトなどで、商品の注文数が書き換えられてしまいます。
否認	否認とは、自分の行った行為を否定するということ。 EC サイトが注文を受付けて商品を配送したのに、 購入者が注文をしたことを否定したり、 個数が違う等の主張をするといったこと。 注文内容が間違いなく Web サイト経由で送られた保証がないと 対処のしようがありません。

現在、クレジットカード番号や個人情報を扱う多くの Web サイトでは、
通信途中での傍受やなりすましによる情報漏洩を防ぐ目的で、**SSL/TLS** を利用しています。

以前から「https」で始まる Web サイトは存在していましたが、
もっぱら個人情報を入力するフォームであるとか、EC サイトにおける商品の入力フォームだけが SSL 化されていました。

かつては、SSL を導入すると暗号化オーバーヘッドのため Web サイトが遅くなるというのが常識でした。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

しかし、サーバー側、クライアント側ともに CPU の性能が向上したことで、
もはやオーバーヘッドはほとんど感じられなくなってきています。

それだけでなく、
SSL 化により HTTP/2 というプロトコルを利用できるようになり、むしろ速くなる
ケースもでてきているそうです。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

2.3 SSL サーバー証明書

SSL/TLS 通信を自分のサイトに実装するには、「**SSL サーバー証明書**」が必要となります。

SSL サーバー証明書とは、
信頼された認証局が情報通信先のサーバーの運営組織が実在していることを証明し、
Web ブラウザと Web サーバー間（サーバー同士でも可能）で
SSL/TLS 暗号化通信を行うための電子証明書のことです。

SSL サーバー証明書には、次の２つの機能があります。

表 2.3-1 SSL サーバー証明書の機能

サイトの実在証明	サイトの運営組織が実在しドメイン名の使用権があることを、信頼される第三者機関が証明します。
SSL 暗号化通信	Web ブラウザと Web サーバー間で暗号化通信を行い、個人情報、クレジットカード番号などが第三者に盗み見られないようにします。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

2.3.1　SSL サーバー証明書の種類（ドメイン認証・企業認証・EV 認証）

ひとくちに**SSL サーバー証明書**といっても、利用用途や費用にさまざまな違いがあります。

（1）独自 SSL と共有 SSL

「**共有 SSL**」とは、
サーバー会社やプロバイダーが代行で取得・所有する **SSL サーバー証明書**を複数の契約者で共有するサービスです。

多くの場合は無料で暗号化通信を手軽に実現することができますが、
共有 SSL の組み込まれたフォームになると URL がプロバイダーのものに切り替わってしまうなど、サイトの利用者からは信頼性に欠ける制限があります。

一方、「**独自 SSL**」は世界的な資格を持った認証局が、
対象のドメイン名に対して専用の **SSL サーバー証明書**を発行して暗号化通信を実現します。

独自 SSL が組み込まれたサイトは、ドメイン名をオリジナルのもので使用でき、
フォームへ移動しても URL は変わりません。

そのほかサイトシールの利用ができるなど、サイトの信頼性をより効果的にアピールできます。

ただし、年間数千円～数万円、
よりセキュリティ信頼度の高い独自 SSL の場合は数十万円の費用がかかります。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

（２）独自 SSL の種類

共有 SSL と比べて信頼度の高い**独自 SSL** ですが、その中にも大きく別けて３つの種類が存在します。

ドメイン認証（Domain Validation: DV）型

ドメインの本当の持ち主であるかどうかを認証します。

個人でも取得可能なので、アンケートや問合せフォームなどに使用されます。

企業認証（Organization Validation: OV）型

ドメインの持ち主であると同時にサイト運営団体の実在性を認証します。
帝国データバンクに企業情報がある法人のみが利用できます。

ネットショップなど個人情報や支払・決済に関する情報を取得するサイトで使用されます。

EV（Extended Validation）

ドメインの持ち主であると同時に、サイト運営団体の実在性を最も厳格に認証します。
帝国データバンクに企業情報があることに加え、企業の活動実態なども審査の対象になります。

知名度の高いブランド・官公庁・教育機関などのサイトで利用されます。

表 2.3-2 独自 SSL の種類

独自 SSL の種類	ドメイン認証型	企業認証型	EV
費用（年）	0～5 万円程度	5 万円～10 万円程度	10 万円～数十万円
取得の審査	易しい	難しい	難しい
信頼度	★☆☆	★★☆	★★★
アピール度	★☆☆	★★☆	★★★
ブラウザでの表示	・鍵マークの表示	・鍵マークの表示 ・企業実在性の証明	・アドレスバーが緑に変化 ・鍵マークの表示 ・企業実在性の証明

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

2.3.2　SSL サーバー証明書の確認方法

ここでは、
Web サイトの SSL サーバー証明書の確認方法を簡単に示します。

Google Chrome と Microsoft Edge についてだけしか示しませんが、
Internet Explorer、Firefox などの他の Web ブラウザでも **SSL サーバー証明書**を確認することができます。
他のブラウザの場合については、検索にてお調べください。

（1）Google Chrome 最新バージョン

今まではアドレスバーの鍵マークをクリックすると、開くダイアログ中に「**証明書の情報**」というメニューがありましたが、
新バージョンからは仕様が変わってこのダイアログの中からメニューが無くなりました。

新バージョンでは、
目的のサイトの **SSL サーバー証明書**は、https から始まる URL の Web サイトにアクセスして以下のいずれかの方法で確認できます。

以下の 3 通りの方法のいずれかで、「**検証**」のウインドウを開きます。

- 「**F12**」キーをクリックする
- 「**Ctrl**」＋「**Shift**」＋「**I**」の各キーを同時にクリックする
- ページ内で右クリック（**図 2.3-1** 参照）の上、「**検証**」をクリックする

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

図 2.3-1 Chrome スクリーンの右クリックメニュー

「**検証**」ウインドウが開いたら、「**Security**」をクリックします。

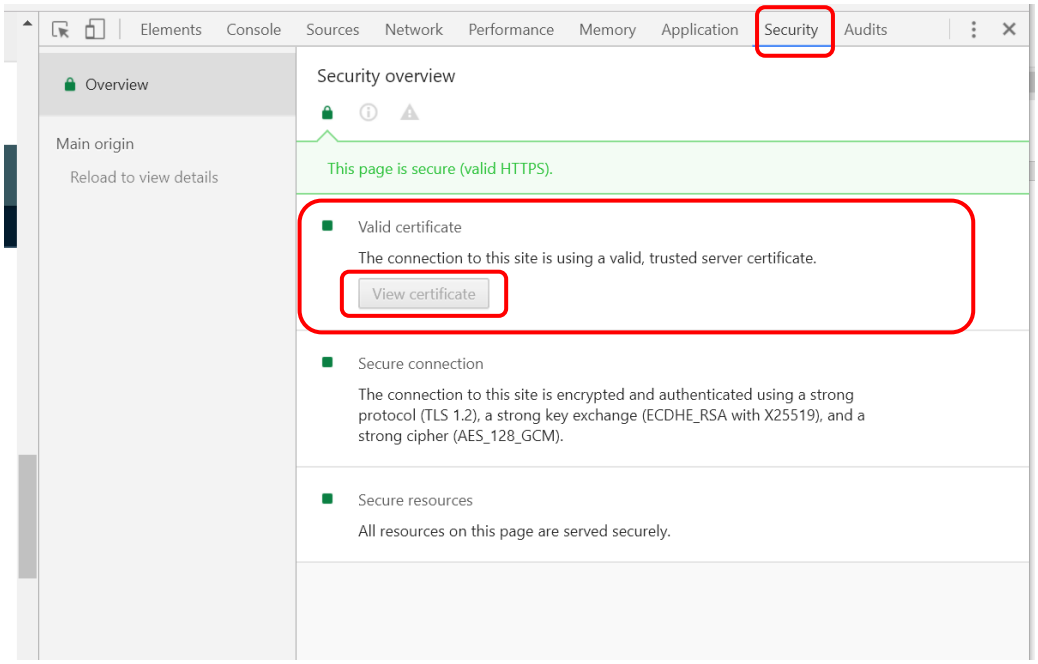


図 2.3-2 検証ウィンドウ

図 2.3-2 に示すように「**Valid certificate**」フィールドの左口が緑色になっていれば、「**View certificate**」をクリックすると図 2.3-3 に示すように **SSL サーバー証明書**の内容が表示されます。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

図 2.3-3 証明書ウィンドウ

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

（２）Windows10 の標準ブラウザである Microsoft Edge。

当たり前のように SSL 通信はできるのですが、今までの Internet Explorer とは違っています。

2017 年 10 月時点での最新のバージョンでは、
組織名や住所情報はもちろんのこと、証明書のウィンドウを表示することができないため、
使われている **SSL サーバー証明書**の詳細を確認することができません。

Edge は、きっと機能向上途中なのでしょう。
SSL サーバー証明書の表示は、セキュリティの上で重要な機能です。
無くてよいわけがありません。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3　無料で利用できる SSL 証明書 Let's Encrypt

通常、HTTPS の Web サイトを運用するには、
商用の認証局に SSL サーバー証明書の発行を申し込み、必ず費用が発生するものでした。

一部限定した目的では無償で利用できるものが用意されており、
サーバーホスティング事業者と認証局との提携（サーバー利用費用に同梱される形など）で
証明書費用が実質かからないサービスのほか、
GMO グローバルサインが 2013 年から行っていたオープンソースプロジェクト向けのプログラムなどがあるくらいでした。

このような状況も、無料の **Let's Encrypt** のサービスが開始されるに伴って変わってきています。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.1 Let's Encypt とは？

Let's Encrypt は、
すべての Web サーバーへの接続を暗号化することを目指したプロジェクトです。

https://letsencrypt.org/

無料だからといって、
信用に足らないといったサービスでは決してありません。

Let's Encrypt の運営母体は、1990 年に設立された
電子フロンティア財団（EFF: Electronic Frontier Foundation）です。

2009 年に制定された長期的なミッションが「ウェブの暗号化（Encrypting the web）」でした。
安全ではない平文の HTTP 通信を、すべて暗号化した HTTPS に置き換えようという野心的な目標が掲げられたのです。

そして、Let's Encrypt Certificate Authority が立ち上がります。
深い知識がなくても、誰もが HTTPS を扱えることを目指しています。
2016 年 4 月 12 日から正式にサービスを開始しました。

非営利団体の ISRG(Internet Security Research Group)が運営しており、
シスコ（Cisco Systems）、**Akamai**、**電子フロンティア財団**（Electronic Frontier Foundation）、
モジラ財団（Mozilla Foundation）といった著名な大手企業・団体が、
ISRG のスポンサーとして **Let's Encrypt** を支援しています。

Let's Encrypt は、支払い、サーバー設定、メールによる確認、証明書の更新といった作業を省略することで、SSL 暗号化における設定や保守の複雑さを大幅に削減することを目的にしています。

完全自動化のため、**ドメイン認証（Domain Validation: DV）型証明書のみ発行**しており、企業認証（Organization Validation: OV）型や EV（Extended Validation）型は提供していません。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

日本語ドメインなどの国際化ドメイン名には、対応しているようです。

https://letsencrypt.org/2016/10/21/introducing-idn-support.html

なお、**Let's Encrypt** は、多くの方が利用している共用型のレンタルサーバーでは現在（2017 年 10 月）のところ利用できないのではないかと思っていますが、
どうなのでしょうか？

導入に際して、SSH などでコマンドをたたく必要があり、
また特定のディレクトリ下のファイルを参照したり、
Apache などの Web サーバーの設定ファイルをいじる必要があるからなのですが。

専用型のレンタルサーバーや VPS では、もちろん利用が可能ですネ。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.2　Let's Encrypt の利用手順

SSL サーバー証明書の取得、そして Web サーバーの SSL 設定は、
非常に煩雑で難しそうに思われている方も多いのではないでしょうか。

Let's Encrypt を利用した場合、
それらはとっても簡単で**図 3.2-1** に示すように全部で 3 ステップしかありません。
また、各ステップも難しい煩雑な作業では決してありません。

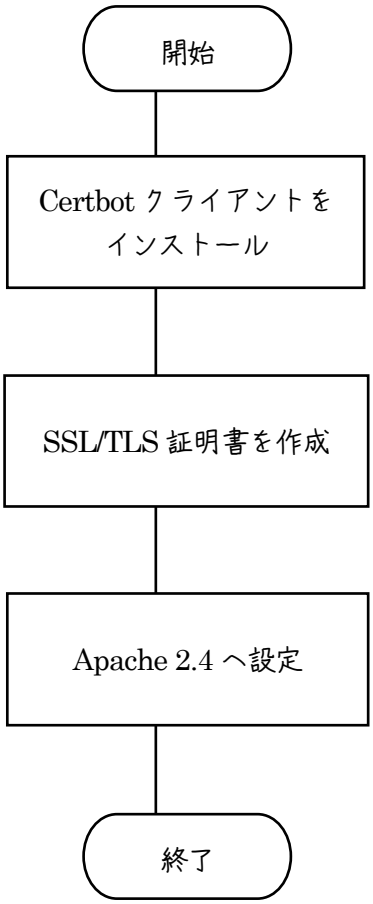


図 3.2-1 Let's Encrypt の導入手順

本書では、**CentOS 7** 上で
Let's Encrypt の **SSL サーバー証明書**を発行して **Apache 2.4** で利用する手順について説明します。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.2.1　事前に行っておくべきこと

Let's Encrypt で発行される証明書は、いわゆる「**DV 証明書**」という種類の証明書です。

Let's Encrypt サーバーは、
発行する証明書の対象のドメインの所有者自身が発行要求をしてきたことを確認した上で、
SSL サーバー証明書を発行します。

具体的にどのようなどのような確認が行われるのかというと、
証明書の発行を要求された **Let's Encrypt** サーバーは、発行しようとしている証明書のドメインの 80 番ポートにアクセスし、特定の内容のファイルが存在していることを確認します。

問題なくファイルが取得できればドメインの所有者が発行要求を出していることを確認できますので、これをもって証明書の発行を行うというわけです。

したがって、
Let's Encrypt の **SSL サーバー証明書**を取得するには、下に示すことがされていなければなりません。
当たり前のことといえば、ごく当たり前の事前条件です。

- Apache 2.4 がすでにインストールされている。
- インターネットから
  HTTP で、80 番ポートで公開しているホームページにアクセスできること。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.2.2　Certbot クライアントのインストール

CentOS 7 用の **Certbot** クライアントは、EPEL リポジトリからインストールすることができます。

次のように epel リポジトリをインストールした上で、
certbot と **python-certbot-apache** をインストールします。

```
# yum install epel-release
# yum install certbot python-certbot-apache
```


Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.2.3　SSL サーバー証明書の作成

SSL サーバー証明書は、
3.2.2 Certbot クライアントのインストールで示した **certbot** クライアントを実行して発行します。

ここでは、Apache httpd の DocumentRoot が「/var/www/www.mywebsite.jp」に設定されていると仮定して話を進めます。
実際の DocumentRoot の設定に合わせて読み替えてください。

（1） certbot クライアント

SSL サーバー証明書を取得するためには、
certbot クライアントは、下に示すように少なくとも次の 2 つのオプションを指定して実行します。

-d オプション	証明書を発行するサーバーのドメイン
-w オプション	DocumentRoot のパスを指定

```
# certbot certonly --webroot -w /var/www/www.mywebsite.jp/ -d www.mywebsite.jp
```

2 つのオプション以外にも、
SSL サーバー証明書の取得に際しては、**表 3.2-1** に示すオプションの利用が可能です。

なお、certbot クライアントの利用可能な全オプションについては、下に示すページをご参照ください。

https://letsencrypt.jp/command/

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

表 3.2-1

オプション	用途
certonly	証明書の取得のみを行います。 デフォルト値は「run」で、 証明書の取得と Apache 等の SSL 設定もやってくれるそうですが、まだうまく動かないことが多いようです。
--webroot	Apache など Web サーバーのドキュメントルートに、 認証用ファイルを生成します。 ドキュメントルート直下に「.well-known/」というディレクトリが作成され、この中に生成されているようです。 稼働している Web サーバーがない場合(メールサーバなど)は 「--standalone」を指定すると良いでしょう。
-w	ドキュメントルートのパスを指定します。 Apache の場合は、DocumentRoot で指定しているパスです。
-d	証明書を取得するドメイン名を指定します。 Apache の場合は、ServerName で指定しているドメイン名です。
-m	ご自分所有のメールアドレスを指定します。 なにかトラブルがあった場合などに Let's Encrypt との連絡用に使用されます。 また、証明書の更新期限が近づくと、ここで指定したメールアドレス宛に、お知らせメールが届きます。
--agree-tos	Let's Encrypt の利用規約に同意します。 利用規約は、下に示すページに記載されています。 https://letsencrypt.org/repository/
-n	「--non-interactive」の省略オプションです。 対話メッセージの表示や入力を求められないようにできます。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

certbot クライアントを起動すると、まず下に示すようにメールアドレスを入力するように求められます。

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel):メールアドレスを入力
```

このメールアドレスは、
後に証明書の有効期限が近づいた際にお知らせしてくれたりすることなどに利用されます。

なお、証明書の有効期間は 90 日間となっています。

次に規約に同意するかを問われます。 同意するために A と入力します。

```
Starting new HTTPS connection (1): acme-v01.api.letsencrypt.org

-------------------------------------------------------------------------------
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.1.1-August-1-2016.pdf. You must agree
in order to register with the ACME server at
https://acme-v01.api.letsencrypt.org/directory
-------------------------------------------------------------------------------
(A)gree/(C)ancel: A
```


Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

次に Electronic Frontier Foundation にメールアドレスを共有するかを問われます。
メールアドレスを共有すると、EFF や証明書のことなどについてのメールを送ると書かれています。
メーリングリストのようなものです。

メールを受け取りたければ Y を、受け取りたくなければ N と入力します。

```
------------------------------------------------------------------------------
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about EFF and
our work to encrypt the web, protect its users and defend digital rights.
------------------------------------------------------------------------------
(Y)es/(N)o: Y
```

これで証明書の作成が開始されます。
正しく証明書の作成が行われた場合は、次のように出力されます。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.mywebsite.jp
Using the webroot path /var/www/www.mywebsite.jp for all unmatched domains.
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/www.mywebsite.jp/fullchain.pem. Your cert will
   expire on 2017-11-19. To obtain a new or tweaked version of this
   certificate in the future, simply run certbot again. To
   non-interactively renew *all* of your certificates, run "certbot
   renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

これで証明書の発行は終了です。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

（２） SSL サーバー証明書が保存される場所

Let's Encrypt で取得する **SSL サーバー証明書**は、
サーバー証明書と**中間 CA 証明書**の２つの証明からなります。

中間 CA 証明書とは、
電子証明書（デジタル証明書）を発行する認証局が、自分自身の認証のために発行する電子証明書の１つです。
「中間証明書」とも言います。
CA とは「Certification Authority」の略で、認証局を意味します。

電子証明書はインターネット上で本人証明を行うために使用されており、
この証明書を発行する「信頼できる第三者」のことを認証局と言います。

他にも、暗号化用の秘密鍵も取得します。

サーバー証明書や秘密鍵は「**/etc/letsencrypt/archive/**」以下に保存され、
表 3.2-2 に示すパスにシンボリックリンクが作成されます。

シンボリックリンクのリンク先は、
SSL サーバー証明書を更新するたびに新しい証明書に変更されます。

表 3.2-2 SSL サーバー証明書の保存パス

ファイル	ファイル・パス
サーバー証明書	/etc/letsencrypt/live/＜ドメイン名＞/cert.pem
サーバー証明書 ＋中間 CA 証明書	/etc/letsencrypt/live/＜ドメイン名＞/fullchain.pem
秘密鍵	/etc/letsencrypt/live/＜ドメイン名＞/privkey.pem
中間 CA 証明書	/etc/letsencrypt/live/＜ドメイン名＞/chain.pem

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

```
# ls -l /etc/letsencrypt/live/www.mywebsite.jp/
total 4
-rw-r--r-- 1 root root 543 Apr 17 17:23 README
lrwxrwxrwx 1 root root 44 Apr 17 17:23 cert.pem -> ../../archive/www.mywebsite.jp/cert1.pem
lrwxrwxrwx 1 root root 45 Apr 17 17:23 chain.pem -> ../../archive/www.mywebsite.jp/chain1.pem
lrwxrwxrwx 1 root root 49 Apr 17 17:23 fullchain.pem -
> ../../archive/www.mywebsite.jp/fullchain1.pem
lrwxrwxrwx 1 root root 47 Apr 17 17:23 privkey.pem -> ../../archive/www.mywebsite.jp/privkey1.pem
```


Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.2.4　Apache 2.4 への設定

SSL サーバー証明書が作成できたら、Apache 2.4 に設定を追加します。

ssl.conf の次に示す項目に、それぞれ設定します。

- SSLCertificateFile
- SSLCertificateKeyFile
- SSLCertificateChainFile

```
[/etc/httpd/conf.d/ssl.conf]
...
SSLCertificateFile /etc/letsencrypt/live/[サーバーのドメイン]/cert.pem
SSLCertificateKeyFile /etc/letsencrypt/live/[サーバーのドメイン]/privkey.pem
SSLCertificateChainFile /etc/letsencrypt/live/[サーバーのドメイン]/chain.pem
...
```

これで Apache httpd を再起動して完了です。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

3.3　SSL 証明書の自動更新

Let's Encrypt の証明書の有効期限は 90 日間と比較的短いため、
定期的に更新する必要があります。

これは自動更新を前提としているためのようです。

自動更新は、「**certbot renew**」コマンドを実行するだけです。
証明書の有効期限をチェックして、期限が近づいていれば更新してくれます。

また、即時に証明書を更新したい場合は「**--force-renewal**」オプションを付けて実行します。
ただし、承認数に上限があるようで、このオプションを付けて毎日コマンドを実行してしまうと、制限に引っかかってしまうようです。
実行するのは月１回程度に制限すると良いでしょう。

手動でコマンドをたたくことは、忘れてしまうこともあり面倒なことでもあるので、
crontab に登録するようにします。

下に示す例は、毎月１日の午前２時に証明書を自動更新し、
Apache をリロードするようになっています。

日本国内向けのサイトであれば、アクセスの少ない午前２時から午前５時の間を選ぶと良いかと思います。

```
0 2 1 * * root /usr/bin/certbot renew && systemctl reload httpd
```


Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

4　AdSense、その他の広告コードの SSL 化対応

HTTPS 経由でアクセスできるサイトでは、
HTTP と HTTPS のコンテンツが混在しているとみなされます。

したがって、HTTPS 対応サイトでは、
広告を含むページ上のすべてのコンテンツが SSL に対応している必要があります。

HTTP の古い広告コードを使用している場合、HTTPS の新しい広告コードに書き換えなければなりません。

本章では、**Google AdSense** をはじめとする主要 ASP の HTTPS 対応状況を整理します。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

4.1　AdSense 用広告コード

AdSense の広告リクエストは、最新のものであれば、基本的に常に SSL に対応しています。
周辺のサイトが HTTP を使用している場合でも、必ず HTTPS 経由で配信されます。

古い AdSense 広告コードを使用している場合は、AdSense スクリプトがブロックされてしまいますので、古い AdSense 広告コードを書き換えなければなりません。

https://support.google.com/adsense/answer/10528?hl=ja

AdSense 広告コードのスクリプトが「http://」で始まっている場合、
「https://」に変更するだけで SSL 化に対応できますが
基本的には下に示すいずれかの手順で対応します。

方法 1:　新しい広告コードを作成する
方法 2:　既存の広告コードを修正する

（1）方法 1: 新しい広告コードを作成する

広告コードを取得し、そのコードをコピーしてから、
広告を掲載するページの HTML ソースコードに貼り付けます。

https://support.google.com/adsense/answer/181960

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

（２）方法 2: 既存の広告コードを修正する

下に示す例のように、スクリプトソースから「http」を削除します。

・同期広告コード

```
<script>
  google_ad_client= “ca-pub-xxxxxxxxxxxxxx” ;
  google_ad_slot= “yyyyyyyyyy” ;
  google_ad_width=300;
  google_ad_height=250;
</script>
<script src="//pagead2.googlesyndication.com/pagead/show_ads.js"></script>
```

・非同期広告コード

```
<script async
src="//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script>
<ins class="adsbygoogle"
  style="display:inline-block;width:300px;height:250px"
  data-ad-client="ca-pub-xxxxxxxxxxxxxx"
  data-ad-slot="yyyyyyyyyy">
</ins>
<script>
  (adsbygoogle=window.adsbygoogle || []).push({});
</script>
```

新しいコードでは、URL は次のように２つのスラッシュで始まります。

同期広告コード:　"//pagead2.googlesyndication.com/pagead/show_ads.js"
非同期広告コード:　"//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

4.2　その他の広告コード

広告コードの SSL 化対応、未対応の判断は、
広告コード（広告スクリプト）の中のリンク・トップが、次のようになっていることでします。

・ 全てのリンクが https:// で始まる　⇒　SSL 化対応

・ ひとつでも http:// で始まっているリンクがある　⇒　SSL 化未対応

当然のことなのですが、
「http://」を「https://」に書き換えたからといって、SSL 化対応の広告コードになるわけではありません。

既にページに貼ってある広告コードが SSL 化未対応の場合、
最新の広告コードを調べ、SSL 化に対応していれば広告コードを貼り替えます。

いくつかの ASP について表 4.2-1 に、SSL 化対応について整理しました。

調べた結果は、ほとんどの ASP が SSL 化を意識し対応しているようなのですが、
弱小の広告主の場合は対応しきれていないというのがざーーっとした印象です。

大手企業の広告に関しては問題が少ないと思いますが、
中小の広告主に関しては自分の Web ページに広告を貼る際、気をつけた方が良いようです。

表 4.2-1

ASP	SSL 化対応	備考
Google AdSense	○	
Amazon アソシエイト	○	
A8 ネット	○	
楽天アフィリエイト	△	基本的には SSL 化に対応していますが、広告主サイトに常時 SSL 化未対応のところがあるようです。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

以上

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

あとがき

本レポートをお読みいただきありがとうございました。

本レポートには Google フォームを使っての簡単なアンケートを下に貼り付けてあります。

もしよければ、ご回答ください。

http://goo.gl/forms/Fu1OFNCtXr

他にご意見、ご質問、ご要望、そして苦情など、メールでも受け付けています。
連絡先は、巻末にあります。

特に、こんなテーマの無料レポートを作成して欲しい、というようなご要望は大歓迎いたします。

よろしくお願いいたします。

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

どっといがの無料レポート

下表は、本レポート以外のどっといがが最近作成した無料レポートの一部です。よければ、こちらの方もお読みいただければと思います。

なお、次のサイトにどっといが作成の全無料レポートのリストがありますので、そちらもご覧ください。

どっといがの無料レポート一覧

作成日	レポート・タイトル	ダウンロード・サイト	概要
2017/07/03	【MailChimp の使い方 Rev. 0.7】 無料で使えるメール配信サービス MailChimp をガッツリ使い倒す！	https://goo.gl/T3kwCH	知らなきゃ損！ 無料から使えるニュースレター（メールマガジン）配信サービス MailChimp がスゴい！ 本レポートは、MailChimp を利用してみたいけど何から始めればいいかわからないという方のために作成しました。
2016/09/10	【無料で独自ドメイン Rev. 2.0】 独自ドメインのブログを 完全無料で開設する！！無料ブログでも AdSense 申請できる？？	https://goo.gl/rYLERc	本レポートでは、 完全無料で独自ドメインのブログを開設する方法をお伝えします。 Rev. 2.0 では、Rev. 1.0 の内容に、Seesaa ブログに無料で独自ドメインを割り当てる方法を追記しました。
2016/09/04	【だれにでもできる 読みやすい文章術】 漢字は開くと、読みやすくなります。でも、やみくもに開けばいいわけではありません。	http://goo.gl/D6Gdv0	Web テキストは、紙に印刷されたものより見やすいとはいえません。 でも、「漢字と仮名（ひらがな、カタカナ）のバランス」を工夫すれば、見づらいという印象を解消することができます。 本レポートでは、どんな場合に漢字で書き、どんな場合にはひらがなで書くべきか、その指針を示します。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

作成日	レポート・タイトル	ダウンロード・サイト	備考
2016/08/27	【Google アナリティクス】 アナリティクスデータを Google マップに表示させる	http://goo.gl/8T5kWp	自分のホームページやサイトがどこからアクセスされているのか、知りたいと思う人も多いのではないでしょうか。実は、アナリティクスのデータは、Google マップに取り込むことができて、Google マップに表示することができるのです。
2016/08/22	【WordPress】 SEO を強化するための 7 つのポイント	http://goo.gl/dNCWfP	インストール直後の WordPress は、そのままでは SEO に強い状態とはいえず、SEO を考慮した設定が別に必要です。 本レポートでは、WordPress のポテンシャルを最大限引き出すために、SEO 効果を高めるための各種設定についてご紹介します。
2016/08/16	【AdSense 検索向け広告の設置】 すこしでも 多くの収益を上げるために！！	http://goo.gl/8pfrD8	Google AdSense の広告には、「コンテンツ向け広告ユニット」の他に、「リンクユニット」や「検索向け広告ユニット」などがあります。 少しでも収益を上げるため、「コンテンツ向け広告ユニット」以外の広告ユニットも利用したいものです。 本記事では、そのうちの「検索向け広告ユニット」の設置方法を、図入りで詳しくお伝えします。
2016/08/08	【驚きの方法】 独自ドメインのブログを 完全無料で開設する！！ 無料ブログでも AdSense 申請できる？？	http://goo.gl/SKxNiv	本レポートでは、 完全無料で独自ドメインのブログを開設する方法をお伝えします。

Copyright (C) 2017 どっといが（五十嵐 康雄） All Rights Reserved.

★どっといがの全無料レポートが自由にダウンロードできます

先の一覧表の無料レポートは、
登録していただくことで自由にダウンロードできるようになります
（一部のレポートについて、将来増補改定し、有料の電子書籍化する予定となっています。 無料で読めるのはここだけ！）。

ご希望の方は、↓このフォームでメールアドレスをご登録ください。

⇒ http://goo.gl/forms/iKxihaFxIF

※ 無料レポートをダウンロードする際には、
Google アカウントへのログインが必要です。

※ Gmail 以外のメールアドレスで登録される場合、
下に示す URL より、
ご希望のメールアドレスと関連付ける Google アカウントを
新しく作成して下さい。

⇒ https://accounts.google.com/signupwithoutgmail

新しく Gmail アカウントを取得する必要はありません。

Google アカウントは、持っていて損になることはありません。

【ご注意】
Google アカウントは、Gmail アカウントと全く同じものではありません（間違って捉えられている方がいらっしゃいます）。

Gmail アカウントは、Google アカウントのうちの一つの種類なのです。

Google アカウント ⊃ Gmail アカウント

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.

発行者情報

◆発行者名

どっといが（五十嵐 康雄）

◆メルマガ情報

【アフィリで稼ぐためのソフトウェア】

サイト運営で使えるWebサービスやソフトウェアを中心に
便利なツール類の使い方を紹介していきます（不定期発行:　情報商材の紹介は、基本的には行いません）。
ニュースレターの解除は、こちら↓

https://goo.gl/cPwQFa

※本レポートをダウンロードされた方は、
自動的にニュースレターへ代理登録されることをご承知おきください。

◆ブログ

サイト運営で使えるWebサービスやソフトウェアを中心に
便利なツール類の使い方を紹介しています。

メインサイト　アフィリで稼ぐためのソフトウェア
サブサイト　Webサービスとソフトウェアの実験室
とほほの初めてのメルマガアフィリ

◆お問い合わせ

freereport@dotiga.jp
or Tohoho.Iga@gmail.com

◆SNS

Twitter　@Tohoho_Iga
Facebook　https://www.facebook.com/dotiga.jp

Copyright (C) 2017　どっといが（五十嵐 康雄）　All Rights Reserved.